JOHN C. ELLIS, JR.
California State Bar No. 228083
REUBEN CAMPER CAHN
California State Bar No. 255158
FEDERAL DEFENDERS OF SAN DIEGO, INC.
225 Broadway, Suite 900
San Diego, California 92101-5030
Telephone: (619) 234-8467/Facsimile: (619) 687-2666
john_ellis@fd.org/ reuben_cahn@fd.org

Attorneys for Ms. Kissane

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

(HONORABLE LARRY A. BURNS)

UNITED STATES OF AMERICA,

Plaintiff,

v.

NICOLE KISSANE,

Defendant.

CASE NO.: 15-CR-1928-LAB

MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF DEFENDANT'S MOTION TO DISMISS COUNTS TWO AND THREE OF THE SUPERSEDING INDICTMENT

I. Introduction

On December 18, 2013, FBI agents seized a TomTom GPS device from Ms. Kissane's car during the execution of a search warrant. The following day, FBI Agent Justin Menolascino brought the TomTom device to the San Diego Regional Computer Forensics Laboratory ("RCFL") to extract data from the device. Although the RCFL has trained forensic analysts, Mr. Menolascino decided to conduct the extraction himself at the RCFL's Cell Phone Investigation Kiosk. *See* Exhibit A (RCFL Cell Phone Investigative Kiosks Brochure). The kiosk is "not designed to take the place of a full-scale [digital device] examination performed by a certified Examiner." *Id.* But it appears to be the only examination performed

here. Moreover, Mr. Menolascino saved some of the data that was extracted, and generated reports, but he did not save all of the files created during the extractions.[1]

Based on the data extracted and decoded by the government, the data shows that the device was near several of the crime scenes. The government's theory is that Ms. Kissane used the device to find the locations and/or had the device in the car during the offenses. Based on the data Mr. Menolascino retained, there is no date and time associated with the locations. In other words, the government claims to have evidence that the TomTom device was near the scene of events, but it cannot tell when it was there. Importantly, had Mr. Menolascino retained all of the data in the appropriate format, Ms. Kissane's expert may have been able to tell the exact date and times the device was near the locations. But Mr. Menolascino's failure to retain all of the data resulted in the destruction of evidence potentially helpful to Ms. Kissane.

Mr. Menolascino's actions gained new significance when the government filed a Superseding Indictment against Ms. Kissane. *See* Dct. No. 124. Counts Two and Three of the Superseding Indictment provide:

> On or about July 15, 2013, within the Southern District of California, defendant NICOLE KISSANE used and caused to be used a facility of interstate and foreign commerce, namely, a TomTom GPS device, for the purpose of damaging and interfering with the operations of an animal enterprise, namely Furs by Graf, a retail furrier located in San Diego, California….

Id. Federal jurisdiction for these local acts of vandalism is premised on the theory that Ms. Kissane used the TomTom device during the events on July 15, 2013.[2]

---

[1] At some point after extracting the data, the FBI returned the TomTom device to Ms. Kissane's mother. The potential forensic value of the device is unknown. The TomTom device is no longer available for retesting by the government.

[2] Ms. Kissane disputes that the use of a TomTom device is sufficient to

But because Mr. Menolascino failed to retain all of the original data from the extractions—resulting in the destruction of data—the defense cannot refute these claims. The appropriate remedy for Mr. Menolascino's actions is dismissal of Counts Two and Three of the Superseding Indictment.

II. Cellebrite Data Extractions

The TomTom device contains a large amount of data. Cellebrite is a company that makes forensic hardware and software that allows for the extraction and decoding of data from digital devices—including Global Positioning System ("GPS") devices like the TomTom. The following sections explain the types of information stored in a TomTom and the way Cellebrite is used to extract and decode this data.

A. Data On The TomTom Device

GPS devices, such as the TomTom XXL, retain a large amount of data. Specifically, forensic extractions of data can yield the following types of data:

- **Favorites.** A user may enter a number of addresses or places into their TomTom and save them as "Favorites." It is then possible for a user to quickly access these places and navigate to them.

- **Home Location.** This is the address or place that has been entered by a user into the TomTom as the location of their home.

- **Recent Destinations.** Recent Destinations are places that the user of the TomTom has selected to navigate to. It does not mean that they have been there, only that the address has been entered.

- **Points of Interest**. Points of Interest are places that are generated either by the user or by the device. They appear in the list of places to which a user can choose to navigate.

---

establish federal jurisdiction, but this is an argument that will be raised during the Fed. R. Crim.Pro. 29 stage if necessary.

- **Entered Locations.** These locations have been entered into the TomTom either as a Home, a Favorite, a Recent Destination, or a Point of Interest. They appear at the top of the list when a user chooses to navigate to a new address.

- **Last GPS Fix.** The TomTom keeps track of the actual location of the device and at random points in time saves its own location. The "last GPS fix" may be along a journey if one is in progress, or just where the device was when it was turned on last.

- **Last Journey Information.** TomTom devices can save the details of the last journey. The last journey "Origin" is the actual position of the TomTom unit. It does not always mean that this is the start of the journey. For example, if the user takes a wrong turn and the TomTom has to recalculate the route, it places the point at which the recalculation occurs as the "Origin" of the last journey. In other words, "Origin" may simply be a place that the TomTom has been physically.

- **Navigated By.** This is how the user selected the location to be stored in the TomTom. When a user selects to navigate to a destination, they can do so by selecting to navigate to:
  - Home
  - Favorite
  - Recent Destination
  - Point of Interest
  - Postal Code
  - Entering the address manually
  - Selecting the point off a map
  - Entering the latitude and longitude
  - Selecting to go to a city center

- **Orphaned Locations.** Orphaned Locations are those addresses found in the deleted space that are no longer part of a file or that are found in the header of a file that has been overwritten. Because they are no longer part of a file, not all the information may be available. Thus, it may not be possible to say what type of entry they are, only that they are present on the device.

See Exhibit B (email from Robert Warren, Senior Tech. Support Rep., Cellebrite).

B. Data Extraction

"Extraction" means copying the data from the device. Generally, there are three types of data extraction that can be performed on a digital device: logical; file system; and physical. *See* Exhibit C, ("What Happens When You Press that Button? Explaining Cellebrite UFED Data Extraction Processes"). For the TomTom XXL, the device examined by Mr. Menolascino, there are only two options: physical and file system. The relevant difference between the two data extractions is that the physical extraction is the most complete, best possible extraction that will obtain more deleted data than a file system extraction. This is the type of extraction performed by Mr. Menolascino.

C. Data Decoding

"Decoding" means the process of converting the data into plain text or another useable format. Cellebrite is a very popular tool for decoding, particularly among law enforcement, because the software turns the extracted data into easy-to-read reports. In other words, the analyst does not have to spend time figuring out what the data means. Or, to put it more precisely, an untrained officer or agent does not have to spend time determining how to interpret the data; certified examiners can (and do) decode additional data, which results in finding more useable information. Here, Mr. Menolascino simply relied on Cellebrite to decode the data from the TomTom device.

III. Extraction, Decoding, and Spoliation of the TomTom Data in this Case

Here, Mr. Menolascino used a Cellebrite product, either the UFED Touch or UFED 4PC,[3] to extract and decode from the TomTom device. Yet he failed to preserve all of the data—including data that is critical to the charges in Counts Two and Three.[4] The resulting spoliation of critical, potentially exculpatory data requires dismissal of Counts Two and Three of the superseding indictment.

---

[3] UFED stands for Universal Forensic Extraction Device.

[4] Ms. Kissane requested all data from the extraction of the TomTom device

The above is a screenshot from Cellebrite that shows the options Mr. Menolascino had for extracting data from a TomTom XXL.

Mr. Menolascino performed numerous physical extractions of the TomTom device. These extractions resulted in files from the device being copied to a media device (*e.g.*, a thumb drive or computer hard drive) at the RCFL. After the extraction, Mr. Menolascino simply relied on Cellebrite to decode the extracted data from the TomTom device, and reduced it to a "report."[5] After Mr. Menolascino extracted and decoded the data from the TomTom device, he made the decision to save some of the files that were acquired during the extraction—and to discard others. One of the files he extracted, but failed to preserve, was the "GPS.bin" file.

/ / /

/ / /

---

months ago. On August 30, 2016, the government advised defense counsel that no additional data existed—which includes the GPS.bin file discussed *infra*.

[5] The report that was produced by Cellebrite in this case is 617 pages. Because of the size, it was not attached as an exhibit, but will be provided to the Court upon request.

As explained by Josiah Roloff, an expert retained by Ms. Kissane to evaluate the government's extraction and decoding of the data, Mr. Menolascino's method resulted in the spoliation of critical data. *See* Exhibit D at 1.[6] Mr. Roloff states:

> Cellebrite extraction report, such as the one generated in this instant case, is simply information the mobile forensic tool manufactured by Cellebrite understands and has been selected by the government examiner to report on. It is by no means, a complete picture of all data that exists on a mobile device. In this specific matter, the government extracted data related to "GPS Fixes", "Journeys", "Locations", and "Data Files". In my review of the extracted data I immediately noted that all reported on GPS coordinates are absent any associated dates and times. Even more alarming, I noted no mention of the device's encrypted "triplogs" and any report regarding an attempt to locate, extract, and otherwise report on them.

Id. at 3-4. Notably, the GPS coordinates and triplog information would have been stored on the GPS.bin file. When the extraction process was complete, Mr. Menolascino should have copied all of the files from the extraction, including the GPS.bin file and all of its contents.

The failure to retain the GPS.bin file and the triplogs information it contained is critical to this case. As Mr. Roloff explains: "In essence, these logs are analogous

---

[6] Mr. Roloff's qualifications include:

- a professional certification in computer forensics from Oregon State University and New Technologies, Inc. (NTI);
- a Certified Computer Examiner (CCE) certification from the International Society of Forensic Computer Examiners;
- an EnCase Certified Examiner (EnCE) certification from Guidance Software;
- a Cellebrite Certified Logical Operator (CCLO) certification and a Cellebrite Certified Physical Analyst (CCPA) certification from Cellebrite; and
- an associate's degree in the applied science of network engineering from Spokane Community Colleges and a bachelor degree in liberal studies with an emphasis in program management from Whitworth University.

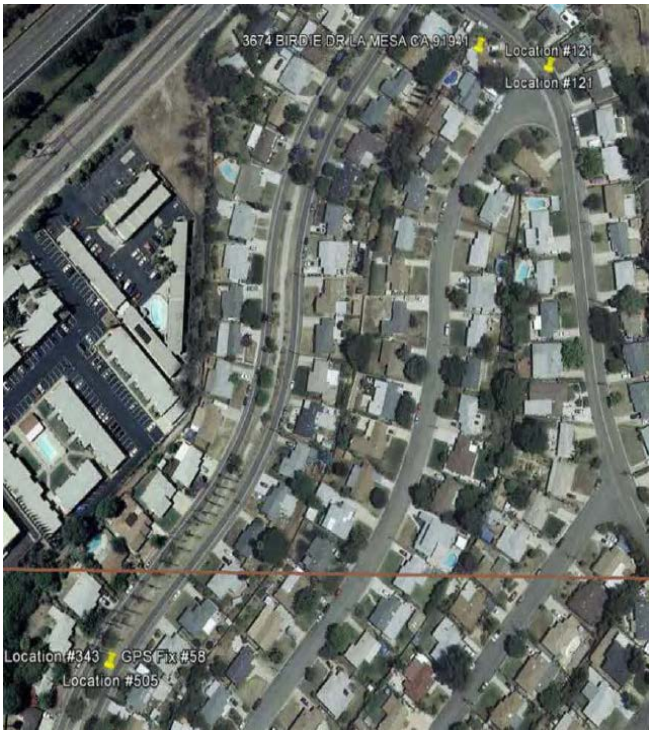
Exhibit D at 1.

to dropping digital breadcrumbs every 1 to 5 seconds as a person drives any particular route." *Id.* at 5. Without retention of the file, there is no opportunity for independent examination of the data to confirm the original examiner's findings or find additional evidence during the decoding process. Mr. Roloff's expert opinion that:

> [w]ithout the government retaining the 2013 extraction or the original device in a manner that would allow for future extractions, the defense is limited to only reviewing the evidence the government decided was relevant to report on. In this case, at a minimum, the defense is missing the opportunity to place context to the GPS coordinates the government has decided are relevant to proving the allegations against Ms. Kissane.

Id.

The government used the data extracted from the TomTom device to create exhibits showing the proximity of locations saved in the device to the homes set forth in Counts Two and Three, such as this one in the this image:



According to the government, the TomTom device was near the home identified in Count Two at some point in time. This, the government posits, proves that Ms. Kissane vandalized the home. But without access to the original data, Ms. Kissane lacks the opportunity to test the government's conclusion because it is impossible to know without the original GPS.bin file whether the device was actually near these locations.

In sum, Mr. Menolascino simply reduced the data extracted from the TomTom device, generated reports, and then returned the original device without

saving all of the data obtained during the extractions. This resulted in spoliation of the data. *See Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec.*, 685 F. Supp. 2d 456, 465 (S.D.N.Y. 2010) (defining spoliation as the destruction or material alteration of evidence or to the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation). And as explained in the following section, it requires dismissal of Counts Two and Three of the superseding indictment.

III. The Appropriate Remedy for the Destruction of Evidence Is Dismissal of Counts Two and Three of the Superseding Indictment

Under the Due Process Clause of the Fifth Amendment, "criminal defendants [must] be afforded a meaningful opportunity to present a complete defense." *California v. Trombetta*, 467 U.S. 479, 485 (1984); *see also United States v. Stever*, 603 F.3d 747, 755 (9th Cir. 2010) ("Whether grounded in the Sixth Amendment's guarantee of compulsory process or in the more general Fifth Amendment guarantee of due process, the Constitution guarantees criminal defendants a meaningful opportunity to present a complete defense.") (internal quotations omitted).

"To safeguard that right," the Supreme Court has "developed 'what might loosely be called the area of constitutionally guaranteed access to evidence.'" *Trombetta*, 467 U.S. at 485 (quoting *United States v. Valenzuela-Bernal*, 458 U.S. 858, 867 (1982)). This access requires, at a minimum, the "deliver[y] [of] exculpatory evidence into the hands of the accused," *Trombetta*, 467 U.S. at 485, and "'the right to put before a jury evidence that might influence the determination of guilt.'" *Stever*, 603 F.3d at 755 (quoting *Pennsylvania v. Ritchie*, 480 U.S. 39, 56 (1987)).

A. The Law on Evidence Destruction

In enforcing the constitutional guarantees of access to evidence and the

opportunity to present a complete defense, the Supreme Court has delineated two lines of authority. On the one hand, when the government destroys "material exculpatory evidence, the good or bad faith of the prosecution is irrelevant: a due process violation occurs whenever such evidence is withheld." *Illinois v. Fisher*, 540 U.S. 544, 547 (2004). In contrast, when the government destroys evidence "'of which no more can be said than it could have been subjected to tests, the results of which might have exonerated the defendant,'" a defendant must establish additional factors to make out a due-process violation. *Fisher*, 540 U.S. at 547-48 (quoting *Arizona v. Youngblood*, 488 U.S. 51, 57 (1988)).

Specifically, the destruction of "potentially useful evidence" – such as the evidence at issue here – rises to the level of a constitutional violation when a defendant can make two showings: (1) "the government acted in bad faith," *United States v. Sivilla*, 714 F.3d 1168, 1172 (9th Cir. 2013) (quoting *United States v. Cooper*, 983 F.2d 928, 931 (9th Cir. 1993)); and (2) "the missing evidence is 'of such a nature that the defendant would be unable to obtain comparable evidence by other reasonably available means.'" *Id*. (quoting *Trombetta*, 467 U.S. at 489).

Recently, in *United States v. Zaragoza-Moreira*, 780 F.3d 971, 977-82 (9th Cir. 2015), the Ninth Circuit clarified the bad-faith inquiry for motions to dismiss based on destruction of "potentially useful evidence." The defendant was arrested with drugs as she tried to cross the border. During her post-arrest interview, she told a duress story and claimed that, while waiting in line, she "tried to attract attention by 'making a lot of noises so I could be noticed,' and by making herself 'obvious.'" *Id*. at 975. In an effort to substantiate her claim, defense counsel asked the government to preserve the video of the pedestrian lanes from the time of the arrest. The government failed to do so, and the defendant moved to dismiss the indictment. The district court denied the motion.

On appeal, the Ninth Circuit determined the video "was not materially exculpatory, but was . . . potentially useful evidence." *Zaragoza-Moreira*, 780

F.3d at 978. It "may have shown [the defendant] throwing her passport on the ground, trying to loosen the packages of drugs from her body . . . [or] other behavior that [defendant] allegedly engaged in to make herself 'obvious' to law enforcement. Such evidence . . . would be particularly helpful to [] establishing . . . her duress claim." *Id.* at 978. And because the evidence was potentially useful, the court turned to the bad-faith inquiry.

As the court explained, "without knowledge of the potential usefulness of the evidence, the evidence could not have been destroyed in bad faith." *Zaragoza-Moreira*, 780 F.3d at 977. Thus, the critical question was whether the government had "knowledge of the potentially exculpatory value of the [evidence] before it was destroyed." *Id.* at 979. In other words, in the destruction of evidence context, bad faith was not a matter of malicious intent, but of knowledge. *See id.* If the government knew the potential usefulness of the evidence but destroyed it anyway, that would establish bad faith. *See id.* The court determined the government had knowledge of the potential usefulness of the evidence because the defendant during the post-arrest interview repeatedly discussed her efforts to attract attention. *Id.* at 979. Thus, the agent's failure to preserve the video was "sufficient to establish bad faith[.]" *Id.* at 981.

The final question, therefore, was "whether the missing evidence is of such a nature that the defendant would be unable to obtain comparable evidence by other reasonably available means." *Zaragoza-Moreira*, 780 F.3d at 981 (internal quotation omitted). The court concluded it was. Only the video could show what actually happened. Thus, the court held that "the district court committed clear error by finding that the apparent exculpatory value of the Port of Entry pedestrian line video was not known to [the agent] and that the government, therefore, did not act in bad faith in failing to preserve the evidence." *Id.* at 982. The conviction was reversed "with directions to dismiss the indictment." *Id.*

B. The Spoliated Data Was Potentially Useful Evidence

The spoliated data on the TomTom device contained potentially useful evidence of which the government had knowledge. Like the video in *Zaragoza-Moreira*, Ms. Kissane cannot refute the government's theory that the TomTom device was used during the offenses without the original data. Indeed, only through examination of the original data could the defense show that the government's theory regarding that Ms. Kissane used the TomTom device in connection with the offense is wrong. Similarly, the original data could show that the TomTom device, and thus Ms. Kissane, were not in the area of the offenses at the time occurred. Thus, without the original data, Ms. Kissane cannot use the device to show a potential alibi. This is the essence of potentially useful evidence because the original data "could have been subjected to tests, the results of which might have exonerated the defendant[.]" *Youngblood*, 488 U.S. at 57); *see also Zaragoza-Moreira*, 780 F.3d at 978. Accordingly, the data falls squarely within the category of "potentially useful evidence," and the government erred in failing to preserve it. *See, e.g.*, Exhibit D at 5.

C. The Government Had Knowledge of the Potentially Exculpatory Value of the Data Before It Was Destroyed, and Thus the Destruction Satisfies the Bad-Faith Requirement

Because the data was potentially useful, the next inquiry is whether its destruction satisfies the bad-faith requirement. The answer turns on whether the government had "knowledge of the potentially exculpatory value of the [evidence] before it was destroyed." *Zaragoza-Moreira*, 780 F.3d at 979.

Here, the government clearly had knowledge that the original data extracted from the TomTom device contained potentially useful evidence. The fact that the data was destroyed by an agent familiar with the facts and evidence is significant. This is not a situation where a government agent or employee accidentally destroyed evidence: Mr. Menolascino's destruction of evidence was intentional.

Thus, the totality of the circumstances establishes that the government knew or should have known of the data's potentially exculpatory value, but destroyed it anyway.[7] Under *Zaragoza-Moreira*, this is the essence of bad faith.

D. There Is No Reasonably Available Comparable Evidence

The final question is whether "the missing evidence is 'of such a nature that the defendant would be unable to obtain comparable evidence by other reasonably available means.'" *Sivilla*, 714 F.3d at 1172 (quoting *Trombetta*, 467 U.S. at 489). On this issue, there can be no debate. Without the data there is no way Ms. Kissane can show that the addresses listed in the TomTom device did not occur on or about the incidents set forth in Counts Two and Three. Nor can she use the data to show that in fact she was not at the charged locations at the time the offenses were committed.

Ms. Kissane's testimony is no substitute. Indeed, the Ninth Circuit rejected that very proposition in *Zaragoza-Moreira*: "The government's argument that in lieu of the destroyed video footage Zaragoza could testify at trial concerning her conduct in the Port of Entry line, runs afoul of Zaragoza's Fifth Amendment right against self-incrimination, by essentially forcing her to testify in her own defense." 780 F.3d at 981.

Similarly, a jury instruction is insufficient to cure the prejudice: "[a] jury instruction [] pales in comparison to the potential value of the actual equipment." *Cooper*, 983 F.2d 932. Consequently, there is no comparable evidence.

/ / /

[7] To the extent the government argues to the contrary, an evidentiary hearing regarding the destruction of evidence is necessary, as occurred in *Zaragoza-Moreira*. *See* 780 F.3d at 979. At such a hearing, Ms. Kissane requests the opportunity to question Mr. Menolascino and all applicable internal government policies regarding evidence preservation.

E. Additional Remedial Measures

Because the deleted data is key to the government's prosecution on Counts Two and Three, the only sufficient remedy is dismissal of the counts. Moreover, the government should also be precluded from entering evidence from the TomTom device for Count One. But if this Court does finds that the destruction of evidence was not in bad faith, suppression of evidence is still warranted. There is no bad faith requirement for granting relief short of dismissal. *See Sivilla*, 714 F.3d at 1173 ("Bad faith is the wrong legal standard for [relief short of dismissal]"). In other words, "[i]f the loss or destruction does not rise to a constitutional violation, relief short of dismissal may be obtained where a balancing of 'the quality of the government's conduct and the degree of prejudice to the accused' favors the latter." *United States v. Zuniga-Garcia*, 472 F. App'x 498, 499 (9th Cir. 2012).

Thus, where the negligent destruction of evidence prejudices the defense, "the court may still impose sanctions including suppression of secondary evidence." *United States v. Flyer*, 633 F.3d 911, 916 (9th Cir. 2011). Here, Because the government spoliated the data, the court should treat the data as if it never existed. That is, all references to the TomTom device should be prohibited.

In the alternative, the court could give "a remedial jury instruction." *Sivilla*, 714 F.3d at 1173. In this case, the instruction should be in the nature of a missing witness instruction – *i.e.*, the spoliated data "'would [have been] unfavorable' to the prosecution." *United States v. Kojayan*, 8 F.3d 1315, n.2 (9th Cir. 1993).

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

IV. Conclusion

The government's destruction of the data from the TomTom device violates Ms. Kissane's due process right to present a complete defense. Because of the nature of the spoliated data coupled with the FBI's practices should result in Counts Two and Three being dismissed.

Respectfully submitted,

Dated: September 30, 2016

s/ John C. Ellis, Jr.

JOHN C. ELLIS, JR.
Federal Defenders of San Diego, Inc.
Attorneys for Ms. Kissane
Email: John_Ellis@fd.org

CERTIFICATE OF SERVICE

Counsel for the Defendant certifies that the foregoing pleading has been electronically served on the following parties by virtue of their registration with the CM/ECF system:

John Parmley
Assistant U.S. Attorney

Michael F. Kaplan
Assistant U.S. Attorney

Respectfully submitted,

Dated: September 30, 2016

s/ John C. Ellis, Jr.
JOHN C. ELLIS, JR.
Federal Defenders of San Diego, Inc.
Attorneys for Ms. Kissane

Email: John_Ellis@fd.org